UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/617,148	07/17/2000	Umesh Maheshwari	07451.0022-00000	8115

7590 06/04/2004	**EXAMINER**
Finnegan Henderson Farabow Garrett & Dunner LLP	GURSHMAN, GRIGORY

Finnegan Henderson Farabow Garrett & Dunner LLP
Erik R Puknys
Stanford Research Center
700 Hansen Way
Palo Alto, CA   94304

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No	Applicant(s)
	09/617,148	MAHESHWARI ET AL.
	Examiner	Art Unit
	Grigory Gurshman	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _4/05/04_.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-23_ is/are pending in the application.
    4a) Of the above claim(s) _16-23_ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-15_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on _17 July 2000_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _5_.
4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1.   Claims 16-23 withdrawn from further consideration pursuant to 37 CFR 1.142(b),

as being drawn to a nonelected method for protecting a database system from external

analysis and attack, there being no allowable generic or linking claim. Applicant timely

traversed the restriction (election) requirement in Paper No. 9.

2.   Applicant's election with traverse of claims 1-15 in Paper No. 9 is acknowledged.

The traversal is on the ground(s) that no additional burden exists for the examiner to

search two groups of claims. This is not found persuasive because, while both groups

of claims are classified in the same class 713, they have acclaimed a separate status in

the art as shown by their different classification in the subclasses. Therefore, a different

and additional search will be required.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter, which the applicant regards as his invention.

4.   Where applicant acts as his or her own lexicographer to specifically define a term

of a claim contrary to its ordinary meaning, the written description must clearly redefine

the claim term and set forth the uncommon definition so as to put one reasonably skilled

in the art on notice that the applicant intended to so redefine that claim term. *Process

Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed.

Cir. 1999). The limitation "hashing the node; encrypting the node; storing the node" in

claims 5, 7 and 9 is used by the claim to mean "hashing the data contained in the node;

encrypting the data contained in the node; storing the data contained in the node". The

term "node" is indefinite because the specification does not clearly redefine the term.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 1-3, 11-15 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Barton (U.S. Patent No. 5.646.997) in view of Honsinger (U.S. Patent

No.6.278.791 B1).

7.   Referring to the instant claims Barton discloses a method and apparatus for

embedding the authentication information within digital data (see abstract). Barton

teaches retrieving meta-data from data block and performing at least one of restoring

step and authenticating step on data block in accordance with meta-data.

8.   Referring to the instant claims, the limitation "receiving a block of data for storage

... " is met by data block in Fig.1. The limitation "generating at least one piece of meta-

data relating to the block of data" is met by meta-data in Fig.1. The limitation

"calculating a first cryptographic hash of at least a portion of the block of data" is met by

calculating signature (see block 10 in Fig.1). The limitation "encrypting the block of data

and encrypting the meta-data to form one or more uniform blocks of encrypted data" is

met by block 16 in Fig.1 and column 3, lines 22-30. The limitation " storing a

cryptographic key in a secret storage medium" is met by authentication bureau (column

5, lines 48-53). Barton, however, does not explicitly teach calculating a cryptographic

hash of the meta-data and comparing the hash values of the meta-data.

9.   Referring to the instant claims, Honsinger discloses lossless recovery of an

original image containing embedded data (see abstract). Honsinger teaches the use of

the hash values of the meta-data. Honsinger teaches that the hash value h is directed

to a hash value comparator circuit 54 where it is compared to the original hash value

recovered from the meta-data. If the hash values are identical, then the recovered

image is declared to be authentic. If they differ, the recovered image (i.e. block of data)

is declared to be altered (see column 9, lines 56-60 and Fig.4). Therefore, at the time

the invention was made, it would have been obvious to one of ordinary skill in the art to

modify the method of retrieving meta-data from data block and performing at least one

of restoring step and authenticating step on data block in accordance with meta-data of

Barton by calculating and comparing the cryptographic hashes of meta-data as taught in

Honsinger. One of ordinary skill in the art would have been motivated to modify the

method of retrieving meta-data from data block and performing at least one of restoring

step and authenticating step on data block in accordance with meta-data by calculating

and comparing the cryptographic hashes of meta-data as taught in Honsinger for

verification of authenticity of received image (see Honsinger, abstract).

10.   Referring to claim 3, Barton teaches that blocks of data are stored in a relational

data-base (see column 2, lines 65-69).

11.   Referring to claims 11 and 14 the limitation "indexing information" is met by the

meta-data, which indexes the file (i.e. data block).

12.   Referring to claim 15, it is well known in the art to use the following types of

computer readable medium: CD-ROM, DVD, MINIDISC, floppy disc, magnetic tape etc.

One of ordinary skill in the art would have been motivated to use these types of

computer readable medium as they are compatible with all of the current computer

systems.

13.   Claims 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Barton (U.S. Patent No. 5.646.997) in view of Honsinger (U.S. Patent No.6.278.791 B1)

an further in view of Hagersten (U.S. Patent No. 5.862.357).

14.   Referring to the instant claims Barton and Honsinger teach creating the uniform

blocks of encrypted data (see Fig.1 of Barton and Fig. 1 of Honsinger). Barton and

Honsinger, however, do not explicitly teach generating a hierarchical location map of

nodes containing the blocks of data.

15.   Referring to the instant claims, Hagersten discloses a symmetrical

multiprocessing system includes a plurality of nodes interconnected by a hierarchical

bus (see abstract). Hagersten teaches a shared memory system including a plurality of

memory locations, wherein the memory locations are allocated to one of a plurality of

processing nodes. The memory locations are configured to be accessed by the plurality

of processing nodes. The system memory locations map to a plurality of address

partitions, whereby the system memory locations are addressed by a plurality of

address aliases, and properties of the address partitions dictate which of the processing

nodes have access to a data request (see column 2, line 53-63 and Fig.1). Therefore,

at the time the invention was made, it would have been obvious to one of ordinary skill

in the art to generate the uniform blocks of encrypted data of Barton and Honsinger and

generate the hierarchical location map of nodes containing the blocks of encrypted data

as taught in Hagersten. One of ordinary skill in the art would have been motivated to

generate the uniform blocks of data and generate the hierarchical location map of nodes

containing the blocks of data as taught in Hagersten for allowing for the transfer of data

between nodes and for restriction of global transfer of local transactions (see

Hagersten, abstract).

16.   Refering to claim 6, the limitation "an indicator specifying the location ... of the

node" is met by TLB (see Fig.1).

17.   Claims 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Hagersten (U.S. Patent No. 5.862.357) in view of Barton (U.S. Patent No. 5.646.997).

18.   Referring to the instant claims, Hagersten discloses a symmetrical

multiprocessing system includes a plurality of nodes interconnected by a hierarchical

bus (see abstract). Hagersten teaches a shared memory system including a plurality of

memory locations, wherein the memory locations are allocated to one of a plurality of

processing nodes. The memory locations are configured to be accessed by the plurality

of processing nodes. The system memory locations map to a plurality of address

partitions, whereby the system memory locations are addressed by a plurality of

address aliases, and properties of the address partitions dictate which of the processing

nodes have access to a data request (see column 2, lines 53-63 and Fig.1).

19.   Referring to claim 7, the limitation "generating a hierarchical location map for

locating individual ones of the plurality of blocks, the hierarchical location map including

a plurality of nodes" is met by system memory locations map (see column 2, lines 53-63

and Figs. 1 and 2). The "location indicators" are met by TLB (see Fig.1). Hagersten

discloses a hierarchical system of location of nodes, but he does not explicitly teach that

node contain the encrypted data.

20.   Referring to the instant claims, Barton discloses a method and apparatus for

embedding the authentication information within digital data (see abstract). Barton

teaches retrieving meta-data from data block and performing at least one of restoring

step and authenticating step on data block in accordance with meta-data. Barton

teaches encrypting the data block (see unit 16 in Fig.1 and column 3, lines 22-30) within

the processor (i.e. node). Therefore, at the time the invention was made, it would have

been obvious to one of ordinary skill in the art to generate the hierarchical location map

for locating the plurality of data blocks residing in the nodes of Hagersten and use

encryption of the data as taught in Barton. One of ordinary skill in the art wouidl have

been motivated to generate the hierarchical location map for locating the plurality of

data blocks residing in the nodes and use encryption of the data as taught in Barton for

enhancing the authentication capability (see Barton, column 4, lines 19-21). Referring to

claims 9 and 10, Barton teaches the use of different cryptographic algorithms as signatures are calculated according the block size (see col.7, lines 14-24).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (703) 306-2900. The examiner can normally be reached on 9 AM-5:30 PM.
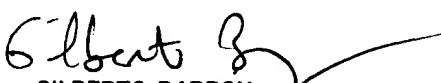
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Grigory Gurshman
Examiner
Art Unit 2132

GG

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100